1:19MJ2109

AFFIDAVIT

I, Paul Cruz, Special Agent of the Federal Bureau of Investigation, United States Department of Justice, being duly sworn on oath, hereby deposes and states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and Federal Rule of Criminal Procedure 41(a)(2)(C), as a Special Agent ("SA") of the Federal Bureau of Investigation. Affiant is empowered to investigate, serve warrants, and make arrests for federal offenses. *See* 18 U.S.C. § 3052.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), Cleveland Division. I have been so employed since 2010 and as such have been assigned to investigate organized criminal enterprises engaged in a variety of racketeering offenses to include drug trafficking, money laundering, document fraud, theft, drug violations, and other criminal offenses which have occurred in, and outside, the Northern District of Ohio. I have training and experience in interviewing and interrogation techniques, arrests, search and seizure, search warrant applications, and various other procedures. In the course of conducting investigations, I have been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses, conducting physical surveillance, consensual monitoring and recording of both telephonic and non-telephonic communications, and executing search warrants. Prior to joining the FBI, I was employed for seven years as a United States Marine Corps officer. In that capacity I was assigned to work investigations involving fraudulent enlistments; fraud against the government; adultery; vehicle accidents; Congressional inquiries; litigation claims; and other crimes under the Uniform Code of Military Justice.

3. The statements contained in this affidavit are based on my personal observations as well as information developed by other SAs of the FBI, United States Secret Service, and officers and detectives of local police departments in Ohio, Georgia, and Florida, who aided in the investigation. Unless otherwise noted, whenever in this affidavit I assert that a statement was made, the information was provided by another law enforcement officer or an investigator (who may have had either direct or hearsay knowledge of the statement) to whom I have spoken or whose report I have read and reviewed. Likewise, any information pertaining to vehicles and registrations, personal data on subjects, and record checks, has been obtained through the Law Enforcement Automated Data System, various state driver's license motor vehicle records, online database searches or the National Crime Information Center computers, and various open source databases such as LexisNexis.

4. Since this affidavit is being submitted for the limited purpose of supporting the application for a criminal complaint in this matter, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that are necessary to establish the probable cause for the issuance of the search warrant sought.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that, as part of a credit card skimming scheme, between in or around May 24, 2014 and on or about January 25, 2019, GUILLERMO VAZQUEZ, WALTER LEYVA ROJAS, LEONDANIS TALAVERA, and others not yet identified, have conspired with each other to commit access device fraud under 18 U.S.C. §§ 1029(a)(2) (obtaining $1,000 in goods with unauthorized access devices in a one-year period), (a)(3) (possessing 15 or more access devices) and (a)(4) (possessing device-making equipment), in violation of 18 U.S.C. §

1029(b)(2), 18 U.S.C. §§ 1028A (Identity theft), and 18 U.S.C. § 371 (Conspiracy) (hereinafter, the "Target Offenses").

BACKGROUND

6. A "skimmer" is an electronic device which can be attached to a point-of-sale credit card reader to covertly copy account information and other data stored on the magnetic strip of a credit or debit card during the payment authorization function which occurs between a merchant and the issuing financial institution during a retail transaction. Credit and debit card account information stored on the skimmer is subsequently copied or transmitted to a computer, either directly, or through a wireless connection.

7. A "credit card reader/writer/encoder" is an electronic device designed to read and rewrite the electronic data contained on the magnetic strip of a credit or debit card. These devices are capable of reading, decoding, verifying and rewriting data on all three "tracks" contained within the magnetic strips on credit cards, debit cards, loyalty cards, gift cards, employee ID cards and electronic hotel room keys. "Track data" includes the cardholder's full name, credit card number, primary account number, card expiration date and country code.

8. A "credit card reader" is similar to a "credit card reader/writer/encoder" but can only read the data contained on the magnetic strip on a credit card or similar type card. When connected to a computer, a card reader enables the user to view and store account and other data contained on the magnetic strip on the card.

9. A "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including a

person's name, Social Security Account number, date of birth, or state or government issued driver's license or identification number.

10. As defined in Title 18, United States Code, Section 1029(e):

(a) "Access Device" includes any card, plate, code, account number, electronic serial number, personal identification number or other means of account access that can be used alone or in conjunction with another access device to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(b) "Counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(c) "Unauthorized access device" means any access device that is lost, stolen, expired, revoked, cancelled or obtained with the intent to defraud;

(d) "Produce" includes design, alter, authenticate, duplicate or assemble;

(e) "Traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

(f) "Device making equipment" means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device.

SKIMMING CASE EXPERIENCE

11. Based on my experience, and the experiences of others from other skimming investigations, I know the following about skimming operations:

a. The suspects operate in small groups to avoid law enforcement detection. There are usually look outs who are in frequent cell contact, prior, and during the fraudulent transactions.

b. The stolen skimming information is usually collected from the areas in which the cloned cards will be used in order to avoid bank fraud notifications of the victims.

c. The skimmers are installed in gas pumps in the vicinity of the fraudulent purchases and are downloaded via Bluetooth technology; this allows the suspects to further avoid law enforcement by not having to open the gas pump up in order to retrieve the skimming device.

d. Skimming suspects usually purchase gift cards with cloned credit cards in order to easily launder the proceeds. Identification need not be shown to use a gift card, and gift cards can be used to make purchases at many retail or other stores. Often, the skimming suspects purchase a small additional personal item, along with the gift cards, to avoid law enforcement or loss prevention suspicion.

e. Often, skimming suspects make fraudulent purchases with cloned cards for personal household items, near their residence; gift cards are purchased away from their residence.

f. The cloned cards are manufactured and encoded with stolen information at a nearby hotel or motel where the suspects can make the cards in privacy without law enforcement detection. The equipment, including skimming devices, computers, and stolen property purchased with the cloned credit cards, is stored in the hotels until they are ready to depart the area. After a sufficient quantity of gift cards purchased with stolen information are acquired, they are mailed or shipped back to their residences, or the residences of the suspect's kin or coconspirators.

g. When skimming suspects are out for the day making fraudulent purchases, they usually keep the bulk of the gift cards that they have purchased and the cloned credit cards they have used or will use to make fraudulent purchases in the vehicle but hidden from plain sight.

h. Often, the fraudulently purchased merchandise, cloned cards, skimming equipment, and computers travel with the suspects to the next hotel where the skimming operation continues in another area.

i. Often, suspects use GPS devices or phones to locate the nearest stores in which to make fraudulent purchases from with cloned cards because they are unfamiliar with the areas in which they conduct their skimming operations.

j. Often the stolen names and credit card numbers obtained through skimming devices are stored on thumb drives.

PROBABLE CAUSE

12. In or around April of 2016, Detective Garth Selong, Rocky River Police Department, began investigating a series of cases involving fraudulent transactions of stolen credit card numbers at retail stores, including big box stores such as Target; Walmart; Sam's Club; K-Mart; and other retail stores throughout the Northern District of Ohio. Detective Selong gathered reports from on or about March 21, 2016 through May 27, 2016, and video surveillances from Rocky River Police Department; Fairview Park Police Department; Strongsville Police Department; Mayfield Village Police Department; Lakewood Police Department; and Medina Police Department. Those police reports detailed approximately 87 fraudulent transactions totaling approximately $14,000 in losses. Detective Selong was able to obtain video surveillance from approximately 50 of those fraudulent transactions, which included three different suspects. Two of the suspects were later identified as Guillermo Vazquez ("VAZQUEZ") and Walter Leyva Rojas ("ROJAS").

13. Flight records from American Airlines states that VAZQUEZ flew from Miami International Airport, to Cleveland, Hopkins Airport on May 1, 2016 and back on May 16, 2016. In that time frame, Detective Selong tracked forty-four (44) fraudulent transactions in five (5) different cities in the Northern District of Ohio for a total loss of approximately $4,500. Seventeen (17) of the fraudulent purchases have video surveillance in which VAZQUEZ, ROJAS, or both are seen using the cloned cards with stolen information encoded.

14. On April 19, 2016, victim MR (real name known to Affiant) filed a complaint with the Rocky River Police Department for unauthorized purchases on his/her credit card. MR confirmed that fraudulent purchases were made at a BJ's Wholesale retail store in Willoughby,

Ohio, on April 15, 2016, as well as other retail stores in the Northern District of Ohio without his/her authorization. Detective Selong requested information on the membership card used to enter the BJ Wholesale store to commit the fraudulent transaction from the senior management at the Willoughby, Ohio, store. The management at BJ Wholesale indicated that the membership card had been opened by ROJAS using his Florida driver's license on April 7, 2016. Additionally, ROJAS added an authorized user of "Guillermo Vazquez," and VAZQUEZ presented his Florida driver's license in order to be added to the account. Surveillance images were obtained from the fraudulent transaction at BJ Wholesale and were compared to the Florida driver's license photos of VAZQUEZ and ROJAS. The images of the suspects are identical to the images of VAZQUEZ and ROJAS in their driver's license photos.

15. During the course of the investigation, Detective Selong contacted Walmart fraud prevention department in order to inquire about a Sam's Club membership card that was used during the course of the fraudulent transactions under the fictitious name "Roberto Perez". According to Walmart fraud prevention, since at least May 24, 2014 until June 18, 2018, fraudulent purchases have been made using stolen credit card numbers, in which the suspects used the Sam's Club membership card "Roberto Perez" to gain access to Sam's Clubs. The suspects made fraudulent purchases at Sam's Clubs and Walmarts using stolen credit card numbers in Ohio; Michigan; Illinois; Colorado; Arizona; New York; Massachusetts; Texas; Washington; and Florida, for a total loss valued at approximately $60,000. The goods purchased mainly consisted of prepaid cards and gift cards. The surveillance images provided by Walmart fraud prevention resemble both VAZQUEZ and ROJAS.

16. On January 25, 2019, a skimming device was located at a gas pump at a Harrison's Tire gas pump in Richmond Hill, Georgia, during a routine examination by the business owner. The business owner called the Richmond Hill Police Department and units were dispatched. The reporting officer examined the skimming device, and discovered "Samsung 8-14" labeled on it. Skimming devices are labeled by the suspects to pair electronic devices via Bluetooth capabilities in order to extract stolen credit card information without having to physically remove the skimming devices and thus avoiding law enforcement detection.

17. Later in the day, on January 25, 2019, during a physical surveillance of the gas pump from which the skimming device was recovered, a Richmond Hill Police Department detective noticed a vehicle parked near the pump. The detective noticed a Hispanic male exit the vehicle and begin to examine the pump without making a purchase. Of note, Harrison's Tire was closed at the time. Additionally, the officer noted the vehicle bore a Florida license plate and ran the license plate for wants and warrants. Before dispatch could report any wants or warrants, the suspect vehicle entered another gas station whereupon the Richmond Hill officers, in a marked unit, exited their vehicle and approached the suspect vehicle for a consensual interview. While one Richmond Hill police officer began a conversation with the driver of the vehicle, the second Richmond Hill police officer noticed, in plain view, the passenger of the suspect vehicle moving retail bags under and behind the seats of the vehicle. The driver of the vehicle explained to the Richmond Hill police officer that the suspects were returning from Kentucky to Florida. The officers allowed the vehicle and the occupants to depart the area. As the suspect vehicle left the second gas station, the Richmond Hill Police officers received a return from dispatch that the suspect vehicle was wanted by the Rincon Police Department,

Georgia, for suspected fraud charges related to skimming. The suspect vehicle was then traffic stopped by the Richmond Hill Police officers where the driver and passenger were asked to exit the vehicle.

18. While exiting the vehicle, the suspects reached for items in their pockets and made movements towards their waist bands. The Richmond Hill Police officers recovered the suspects' wallets and located their driver's licenses, which identified them as VAZQUEZ, passenger, and Leondanis Talavera ("TALAVERA"), the driver. After the suspects were removed from the vehicle, a K-9 unit conducted a scan on the outside of the vehicle and detected the presence of the odor of narcotics during the K-9's scan. Richmond Hill Police Officers obtained verbal consent to search the vehicle from VAZQUEZ and TALAVERA. During the search of the vehicle a silver colored laptop computer HP Envy Notebook PC, Model 15-as020nr, Serial Number 5CG718076J; black and red Sandisk thumb drive Glide 32 GB, serial BM180625881B; SIM card, S/N: 890102608955160080991; retail items; receipts including Walmart and Lowes stores; and gift cards were recovered from the passenger side of the vehicle. Additionally, a pry bar; epoxy; multi-tool; gloves; eight (8) credit cards with zip codes written on the back embossed with the name "William Vazquez"; and gas pump seals were recovered near the passenger seat. The gas pump seals are used to maintain the integrity of the gas pump, bearing the gas station warning emblem, in order for customers to detect tampering of the seals. Furthermore, black front and white back, Apple I-Phone, Model X-Plus, and a black Samsung phone, Galaxy Note 8, with cracked screen (note that "Samsung 8-14" was written on the recovered skimming device), and a modified USB cable for a skimming device, were also

recovered in the vehicle. A local search warrant issued in Bryan County, Georgia, was obtained by Richmond Hill Police Department for the electronic devices.

19. Special Agent Jason Lynch, Secret Service, Savanah Division, obtained copies of the receipts recovered during the traffic stop and search by Richmond Hill Police Department. SA Lynch obtained the actual credit card numbers encoded on the recovered credit cards. SA Lynch identified the victims associated with the stolen credit card numbers and traced several fraudulent transactions. Of note, surveillance videos from Walmart on September 17, 2018; September 18, 2018; September 19, 2018; November 9, 2018; December 2, 2018; December 4, 2018; and December 14, 2018; in Rincon, Georgia, depict VAZQUEZ and TALAVERA using cloned credit cards with the stolen information encoded to make fraudulent purchases. There was approximately $12,000 in loss to the victims for those fraudulent purchases. Additionally, surveillance stills were captured from a Lowes hardware store on January 25, 2019, in which VAZQUEZ is making fraudulent purchases. The receipts of the purchases matches the retail items recovered during the search.

20. On February 7, 2019, Richmond Hill Police Department, conducted a cursory search of the Samsung Note 8 cell phone. The search revealed a pinned location, obtained from a picture of a skimming device labeled “Samsung 8-16” at a Citgo gas station located in Pooler, Georgia. In January 2019, Pooler Police Department reported that they recovered a skimming device from the Citgo gas station with the marking “Samsung 8-16” consistent with the picture viewed on the suspect’s phone.

21. On March 26, 2019, a federal search warrant was issued and executed in the Northern District of Ohio for electronic devices that were seized on January 25, 2019, during the

traffic stop of VAZQUEZ and TALAVERA. During the execution of the search warrant it was discovered that on the Samsung Note 8, the phone number "305-766-8575" was assigned to the phone. Additionally, a search of the SIM card revealed that the phone number "786-853-5345" was assigned to the SIM card. The I-Phone X IMEI No. 357264090791089, contained multiple pictures of VAZQUEZ, and was assigned phone number "786-531-5424". Also during the execution of the search warrant, the stolen names and credit card numbers of approximately 2,400 victims were identified on the Sandisk thumb drive and computer. Additionally, software used to encode the cloned credit cards was found on the seized thumb drive and computer. Furthermore, pictures and geolocations recovered during the execution of the search of the I-phone and Samsung phones showed that the suspects were frequenting gas stations and retail stores in multiple states to continue to facilitate the fraud scheme.

22. During the search of the cell phones, a number of pictures of Western Union transfers were located. The pictures were taken by the suspects as a way to track the laundering of the stolen proceeds and maintain accountability of the stolen gift card values. There were also a number of pictures of retail items and gift cards taken during their "shopping trips." Not all of the pictures have a geo-locate tag making it impossible to identify where the pictures were taken without identifying the cell sites in which the suspects hitting off during their trips. There was one Western Union money transfer from VAZQUEZ to TALAVERA.

23. In the "notes" section of the phone belonging to VAZQUEZ, VAZQUEZ stored a series of references to gas station locations as well as the number on the skimming device that the gas stations paired with. For example, "Exxon s el numero 8" and "La bomba cigo el nemero 16". Translated to "#Exxon (gas station) the number 8", and "the beeper Citco (gas

station) the number 16". From experience, the word "beeper" is used for code for a skimming device.

24. Additionally, during the search of the cell phones, a video was viewed of a suspect prying open a gas pump in order to extract a skimming device.

25. A number of text messages and chats were also discovered during the execution of the federal search warrant on the I-Phone X belonging to VAZQUEZ. Of note, the text messages were sent from "Leo" TALAVERA to VAZQUEZ of locations of gas stations in Georgia, including the Pooler gas station in which a skimming device was recovered.

26. On April 5, 2019, a federal search warrant was issued in the Northern District of Ohio for historical cellular sites on the phone numbers associated with the phones recovered during the traffic stop on January 25, 2019, in Richmond Hill, Georgia. On April 15, 2019, the cell sites were plotted for a phone number associated with VAZQUEZ's phone. The date range was November 11, 2018 through January 25, 2019. When a cell phone places a call or text, it connects to a cell phone tower in the vicinity commonly referred to as a "hit". On November 19, 2018, VAZQUEZ's phone hits off of cell site towers from Miami, Florida, which travels to Richmond Hills and Pooler, Georgia, then returns to Miami, Florida. On November 29, 2018, VAZQUEZ's cell phone hits off of cell site towers from Miami, Florida back which travels to Richmond Hills and Pooler, Georgia, near the locations of the gas stations in which skimming devices were recovered. On November 20, 2019, VAZQUEZ's cell phone hits off of towers in Savanah, Georgia, then returns to Miami, Florida. On November 14 and 25, 2018, and January 25, 2019, the same pattern of VAZQUEZ's cell phone hits off towers departing from Miami,

Florida, and traveling to areas new the Richmond Hill and Pooler gas stations in which skimming devices were recovered.

27. On April 17, 2019, the cell sites were plotted for a phone number associated with TALAVERA's phone. The data range was April 10, 2017 through January 25, 2019. On August 7, 2018, TALAVERA's cell phone hits off towers from Miami to Richmond Hill, Georgia, gas station, and then returns to Miami on August 8, 2018. The same pattern of TALAVERA's cell phone hits off towers departing from Miami, Florida, and traveling to Richmond Hill gas station in which a skimming device was recovered. On October 4, 2018, December 2, 2018, and January 25, 2019, TALAVERA's cell phone hits off towers departing from Miami, Florida, and travels to the vicinity of the Pooler gas station in which a skimming device was recovered.

17. On March 28, 2019, I received and email from Special Agent Todd Porinsky ("Porinsky"), United States Secret Service ("USSS"), in regards to VAZQUEZ and ROJAS. Porinsky provided surveillance excerpts from the USSS in 2017. On May 23, 2017, physical surveillance was conducted on VAZQUEZ. During the surveillance, VAZQUEZ was seen tampering with two (2) pumps at an Exxon gas station located in Diana Beach, Florida, and another pump at a Chevron gas station, in Miami Lakes, Florida, but was unsuccessful in installing skimming device. On June 5, 2017, a federal search warrant in the Southern District of Florida was issued for a tracking device to be placed on a BMW driven by VAZQUEZ. On June 25, 2017, VAZQUEZ was seen entering several Walmarts in the Miami area and used several credit cards per location. Surveillance video from the fraudulent purchases was recovered by the USSS

and placed into evidence. Additionally, USSS agents spoke with loss prevention specialist at each Walmart and determined that all the transactions that VAZQUEZ made were fraudulent.

18. On July 8, 2017, a similar physical surveillance was conducted on VAZQUEZ. VAZQUEZ was seen entering several Walmarts and conducting more fraudulent transactions. After the fraudulent transactions occurred, the Coral Springs Police Department conducted a traffic stop for vehicle violations. During the routine traffic stop, Coral Springs Police Department positively identified VAZQUEZ and he was issued a warning for the traffic violation.

19. On July 13 and 15, 2017, a similar physical surveillance was conducted on VAZQUEZ, where VAZQUEZ made several fraudulent purchases from Walmarts in the Miami, Florida area.

20. In April 2019, I reviewed records from Squared Inc., a service provided to merchants to establish a mobile payment account. The records stated that card usage included activity that was not consistent with legitimate usage. Nearly all of the activity of the payment accounts were done often occurred back-to-back in a rapid manner. Square Inc. provided documentation that two (2) accounts belonging to TALAVERA, and one (1) account belonging to an associate of TALAVERA, attempted 241 transactions; 104 which were declined, for an attempted loss amount of approximately $15,000. Of the $15,000, approximately $7,100 was successfully processed. The successful transactions were deposited into two bank accounts belonging to an associate of TALAVERA and two bank accounts belonging to TALAVERA.

CONCLUSION

21. Based on the foregoing facts, your Affiant respectfully submits that there is probable cause to believe that GUILLERMO VAZQUEZ, WALTER ROJAS and LEODANIS

TALAVERA, have conspired to committed access device fraud and identity theft from at least May 24, 2014 to January 25, 2019.

22. Your Affiant respectfully requests that the Court issue arrest warrants for the GUILLERMO VAZQUEZ, WALTER ROJAS, and LEODANIS TALAVERA

Respectfully submitted,

Special Agent Paul Cruz
Federal Bureau of Investigation

Sworn to via telephone after submission by reliance electronic means.
Fed. R. Crim. P. 4.1 and 41(d)(3).

This 3rd day of May, 2019.

DAVID A. RUIZ
United States Magistrate Judge